AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated in the following listing of all claims:

1. (***Cancelled***)

2. (***Cancelled***)

3. (*New*) A method for coordinating update of certificate revocation information in a distributed public key infrastructure (PKI) environment, the method comprising:

receiving a delta coded update to a certificate revocation list (a delta CRL) together with an associated first hash value, the delta CRL encoding an update to a preceding certificate revocation list state CRL(t) and the first hash value computed as a function of at least a resultant state CRL(t+n) computable by applying the delta CRL to the CRL(t) state;

computing an update to a local certificate revocation list state by applying the received delta CRL to produce a resultant local CRL state; and

validating the update at least in part by computing a second hash value as a function of at least the resultant local CRL state and comparing the second and first hash values.

4. (*New*) The method of claim 3, further comprising:

requiring, as a condition precedent to the update, that a transmission that conveys the delta CRL include a valid digital signature establishing a trusted source thereof.

5. (*New*) The method of claim 3, further comprising:

wherein the first hash value is computed as a function of both the CRL(t) and CRL(t+n) states, and

wherein the second hash value is computed as a function of both a prior local CRL state and the resultant local CRL state.

6. (*New*) The method of claim 3, further comprising:

requesting a CRL update, the request indicating a base t beyond which update is desired; and

receiving in response to the request, plural delta CRLs including the first delta CRL and at least one other delta CRL together with respective associated hash values including the first hash value and at least one other hash value, wherein each hash value is computed as a function of a respective resultant certificate revocation list (CRL) state.

7. (*New*) The method of claim 6,

wherein each of the hash values is computed as a function of both a respective prior CRL state and the respective resultant CRL state from which the associated delta CRL is derived.

8. (*New*) The method of claim 6, further comprising:

performing successive updates to the local certificate revocation list state by applying successive ones of the delta CRLs received in response to the request; and

validating the successive updates based on the respective associated hash values.

8. (*New*) The method of claim 6,

wherein the base t is a temporal index.

10. (*New*) The method of claim 3, further comprising:

if the validating is unsuccessful, requesting a complete copy of a current certificate revocation list.

11. (*New*) A method for coordinating update of certificate revocation information in a distributed public key infrastructure (PKI) environment, the method comprising:

preparing a first delta coded update to a certificate revocation list (a first delta CRL), the first delta CRL encoding an update sufficient to produce a subsequent certificate revocation list state CRL(t+n) from a preceding certificate revocation list state CRL(t);

computing an associated first hash value as a function of at least the CRL(t+n) state; and

transmitting the delta CRL and the associated first hash value in response to a request for certificate revocation list update beyond a base t.

12. (*New*) The method of claim 11,

wherein the first hash value is computed as a function of both the CRL(t) and CRL(t+n) states.

13. (*New*) The method of claim 11, further comprising:

receiving a CRL update request indicating a base t beyond which update is desired; and

transmitting in response to the request, plural delta CRLs including the first delta CRL and at least one other delta CRL together with respective associated hash values including the first hash value and at least one other hash value, wherein each hash value is computed as a function of at least a respective resultant certificate revocation list (CRL) state from which the associated delta CRL is derived.

14. (*New*) The method of claim 13,

wherein each of the hash values is computed as a function of both a respective prior CRL state and the respective resultant CRL state from which the associated delta CRL is derived.

15. (*New*) The method of claim 13, further comprising:

performing successive updates to the local certificate revocation list state by applying successive ones of the delta CRLs received in response to the request; and

validating the successive updates based on comparison of the associated hash values with respective locally computed hash values.

16. (*New*) A system comprising:

first and second validation authorities (VAs) communicatively coupled to propagate certificate revocation list (CRL) information;

the first VA configured to prepare delta CRLs in correspondence with updates from a certificate authority (CA), each delta CRL encoding a respective update sufficient to produce a next certificate revocation list state CRL(t+n) from a preceding

certificate revocation list state CRL(t), the first VA further configured to compute respective first hash values as a function of respective sequentially adjacent pairs of states CRL(t) and CRL(t+n); and

the second VA configured to receive the delta CRLs from the first VA, to calculate based thereon updates to local certificate revocation list states by applying the received delta CRL to produce a resultant local CRL state, and to validate each update based at least in part on comparison of respective first hash values received from the first VA with second hash values computed as a function of respective prior local CRL states and resultant local CRL states.

17. (*New*) The system of claim 16,

wherein transmission of a given delta CRL and its associated first hash value are secured using a digital signature.

18. (*New*) The system of claim 16,

wherein the delta CRLs and associated first hash values are received via an intermediary.

19. (*New*) A computer program product encoded in one or more media and including instruction sequences executable on a processor of a system that hosts a validation authority to perform the receiving, computing and validating steps of claim 3.

20. (*New*) A computer program product encoded in one or more media and including instructions sequences executable on a processor of a system that hosts a validation authority to perform the preparing, computing and transmitting steps of claim 10.

21. (*New*) A computer readable encoding of a delta CRL, the computer readable encoding encoded, at least transiently in a medium, and comprising:

delta coded certificate revocation list (CRL) update data that allows a receiving validation authority to generate an updated CRL by applying the delta coded CRL update to a previous CRL state;

a self-validating indicator encoded in association with the delta coded CRL update, the self-validating indicator encoding a hash computed not as a function of the delta

coded CRL update itself, but rather as a function of the next certificate revocation list state CRL(t+n) which may be generating by applying the delta coded CRL update to a previous certificate revocation list state CRL(t); and

a digital signature establishing identity of a source of the computer readable encoding.

22. (*New*) The computer readable encoding of claim 21,

wherein the encoded hash is computed as a function of both the next state CRL(t+n) and the previous state CRL(t).